Privacy Impact Assessment

for the

Chemical Facility Anti-Terrorism Standards Program Suspicious Activity Reports

DHS Reference No. DHS/CISA/PIA-036

December 16, 2020

Homeland Security

Abstract

The Cybersecurity and Infrastructure Security Agency (CISA) Infrastructure Security Division (ISD) Chemical Security Subdivision, hereafter referred to as Chemical Security, receives notification of security incidents at high-risk chemical facilities. This Privacy Impact Assessment (PIA) describes the incident and suspicious activity reporting actions previously performed by CISA's legacy National Infrastructure Coordinating Center (NICC)[1] and now performed by Chemical Security. This PIA outlines the personally identifiable information (PII) that CISA routinely receives when evaluating information about security incidents and their potential nexus to terrorism and replaces the DHS/NPPD/PIA-017 NICC Suspicious Activity Report (SAR) PIA.[2]

Overview

On October 4, 2006, the President signed the U.S. Department of Homeland Security Appropriations Act of 2007 (the Act), Pub. L. No. 109-295. Section 550 of the Act provided the U.S. Department of Homeland Security (DHS or the Department) with the authority to regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the Chemical Facility Anti-Terrorism Standards (CFATS) Interim Final Rule (IFR) implementing this statutory mandate.[3]

The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014,[4] commonly referred to as the CFATS Act of 2014,[5] replaced section 550 and codified the CFATS program into the Homeland Security Act of 2002.[6] On July 22, 2020, the President signed into law an Act to extend the CFATS program until July 27, 2023.[7] CISA is responsible for implementing CFATS on behalf of the Department.

A high-risk chemical facility is one that the CISA's Chemical Security identifies as a

[1] The legacy NICC's functions were integrated into CISA Central as of June 3, 2020. More information on CISA Central can be found at https://www.cisa.gov/central.
[2] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, PRIVACY IMPACT ASSESSMENT FOR THE NATIONAL INFRASTRUCTURE COORDINATING CENTER SUSPICIOUS ACTIVITY REPORTING INITIATIVE, DHS/CISA/PIA-017 (2010 and subsequent updates), *available at* https://www.dhs.gov/privacy-documents-cisa.
[3] *See* 72 Fed. Reg. 17688 (Apr. 9, 2007) at https://www.federalregister.gov/documents/2007/04/09/E7-6363/chemical-facility-anti-terrorism-standards.
[4] The Protecting and Securing Chemical Facilities from Terrorist Attacks Act of 2014 (Pub. L. No. 113-254) codified the CFATS program into the Homeland Security Act of 2002. *See* 6 U.S.C. 621 *et seq.*, as amended by Pub. L. No. 116-2, § 2, 133 Stat. 5 (2019); Pub. L. No. 116-136, div. B, title VI, § 16007, 134 Stat. 546 (2020); Pub. L. No. 116-150, § 1(a), 134 Stat. 679 (2020).
[5] Pub. L. No. 113-254 (2014).
[6] *See* 6 U.S.C. 621 *et seq.*
[7] Pub. L. No. 116-150 (2020).

chemical facility of interest (CFOI) and meets the risk criteria developed under 2102(e)(2)(B) of title XXI of the Homeland Security Act of 2002 (as amended).[8] If a facility is determined to be high-risk, the facility must implement a Site Security Plan, Expedited Approval Program, or Alternative Security Program, which must be approved by CISA. As a part of the approved security plan, high-risk chemical facilities are required to notify CISA of security incidents.

When Chemical Security receives information about a security incident, its focus is whether the security incident at the chemical facility is satisfactorily resolved and then whether the facility complied with its regulatory obligations. The security incidents are generally documented in an "Incident Report" by Chemical Security Inspectors (CSIs) and transmitted through Supervisory CSIs via email to Chemical Security for review; Chemical Security maintains a log of each security incident for tracking and metrics. Each incident is reviewed by Chemical Security and assigned a unique identifier (one that is unrelated to PII) for internal tracking. The incident information is subsequently stored in an access-restricted shared drive to which only those individuals who work within Chemical Security, have an official "need to know," and have responsibilities for handling incident reports may gain access.

Chemical Security follows the Nationwide SAR Initiative (NSI),[9] evaluating security incidents in light of the Information Sharing Environment (ISE) SAR Functional Standard.[10] Those Chemical Security personnel involved in evaluating security incidents for consideration as an ISE-SAR, will be properly trained in accordance with criteria in the ISE-SAR Functional Standard and on the requirements to comply with NSI. A trained Chemical Security personnel member will review the incident information and exercise personal judgment, based upon a combination of knowledge, experience, and available information, to determine whether the information has a potential nexus to terrorism. Only those incidents that meet the ISE-SAR Functional Standard will be submitted directly into the Nationwide SAR Initiative SAR Data Repository (i.e., eGuardian[11]).

Chemical Security will also review eGuardian submissions to identify other incidents reported by law enforcement that have likely occurred at or near high-risk chemical facilities or involve chemicals that could be used for terrorist purposes. When a potential chemical facility-

[8] *See* Homeland Security Act at https://www.govinfo.gov/content/pkg/CPRT-114HPRT99615/html/CPRT-114HPRT99615.htm.

[9] The NSI is a joint collaborative effort by DHS, the Federal Bureau of Investigation (FBI), and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with another tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing SAR information. Information about NSI may be found at https://www.dhs.gov/nsi.

[10] The ISE SAR Functional Standard incorporates key elements that describe pre-operational behaviors that are criminal in nature and have historically been associated with terrorism. *See* the ISE SAR Functional Standard at https://www.dhs.gov/publication/ise-sar-functional-standard.

[11] *See* U.S. DEPARTMENT OF JUSTICE, FEDERAL BUREAU OF INVESTIGATION, PRIVACY IMPACT ASSESSMENT FOR THE eGuardian SYSTEM, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/eguardian-threat.

related incident within eGuardian is identified, Chemical Security will contact the reporting law enforcement agency and confirm whether the incident does or does not relate to a high-risk chemical facility.

- If the incident does pertain to a high-risk chemical facility, Chemical Security first will coordinate with the respective law enforcement agency that has jurisdiction in that area/location, and then when authorized by that law enforcement agency, Chemical Security will coordinate with the high-risk chemical facility to ensure its compliance with CFATS.
- If the incident does not pertain to a high-risk chemical facility but indicates the possibility for a Potential CFOI, Chemical Security first will coordinate with the law enforcement agency and then perform operational deconfliction.
- If the incident does not indicate the involvement of a high-risk chemical facility nor a Potential CFOI, no further action will be taken by Chemical Security.

Chemical Security primarily receives incident reports about chemical facilities from regulated facilities themselves, as required under 6 C.F.R. § 27.230(a)(15). These reports can include the PII of individuals reported as being involved in suspicious activities at or near a high-risk chemical facility, as well as the PII of individuals who report suspicious activities.

CISA seeks to ensure that the security incidents at high-risk chemical facilities are fully evaluated and acted upon. This PIA describes how Chemical Security receives and evaluates such security incident reports, and the additional actions Chemical Security takes to add value before passing the security incident on for evaluation by law enforcement. Chemical Security does not perform this activity for other critical infrastructure sectors or for facilities that do not possess chemicals.

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or agreements permit and define the collection of information by the project in question?

Section 550 of the Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295 (2006) ("Section 550"), provides the Department with the authority to identify and regulate the security of high-risk chemical facilities using a risk-based approach. On April 9, 2007, the Department issued the CFATS IFR implementing this statutory mandate.[12]

The CFATS Act of 2014, Pub. L. No. 113-254, replaced Section 550 of the DHS

[12] *See supra* note 3.

Appropriations Act of 2007 and codified the CFATS program into the Homeland Security Act of 2002.[13] CISA/ISD is responsible for implementing CFATS on behalf of the Department.

CISA has the authority to share information under 6 U.S.C. § 652(e)(1)(H) to assist in the deterrence, prevention, or preemption of, or response to, terrorist attacks against the United States.

1.2 What Privacy Act System of Records Notice(s) (SORN(s)) apply to the information?

The information collected by this project is currently covered under DHS/NPPD-001 – National Infrastructure Coordinating Center (NICC) Records SORN.[14] CISA intends to publish a new CISA-wide SORN to describe SAR activities. When the CISA-wide SORN is published in the *Federal Register* and becomes effective with similar Privacy Act Exemptions, this PIA will be covered under the new CISA-wide SORN.

1.3 Has a system security plan been completed for the information system(s) supporting the project?

There is not a system security plan as the receipt of incident information is done primarily via email.

1.4 Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

Yes. Records created by CISA, such as the security incident reports, are considered official communications and thus covered under the General Records Schedule DAA-0563-2013-0002-0002 and retained for seven years.[15] If the security incident meets the ISE SAR Functional Standard and is submitted into eGuardian, then the record retention schedule for the SAR will be governed by the record retention schedule applicable to eGuardian.[16]

---

[13] *See* 6 U.S.C. 621 *et seq.*, as amended by Pub. L. No. 116-2, § 2, 133 Stat. 5 (2019); Pub. L. No. 116-136, div. B, title VI, § 16007, 134 Stat. 546 (2020); Pub. L. No. 116-150, § 1(a), 134 Stat. 679 (2020).

[14] *See* DHS/NPPD-001 National Infrastructure Coordinating Center (NICC) Records System,76 Fed. Reg. 55693 (Sept. 8, 2011), *available at* https://www.dhs.gov/systemrecords-notices-sorns.

[15] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER DAA-0563-2013-0002-0002, U.S. DEPARTMENT OF HOMELAND SECURITY, SITUATIONAL REPORTS, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-homeland-security/rg-0563/daa-0563-2013-0002_sf115.pdf.

[16] *See* NATIONAL ARCHIVES AND RECORDS ADMINISTRATION, REQUEST FOR RECORDS DISPOSITION AUTHORITY, RECORDS SCHEDULE NUMBER N1-065-11-040, U.S. DEPARTMENT OF JUSTICE, GAURDIAN THREAT TRACKING SYSTEM, *available at* https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-justice/rg-0065/n1-065-11-040_sf115.pdf.

1.5 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

The information collected by this project is not covered by the PRA because it does not qualify as an information collection under 5 C.F.R. § 1320.

Section 2.0 Characterization of the Information

2.1 Identify the information the project collects, uses, disseminates, or maintains.

This project receives PII primarily about two categories of individuals: (1) those who submit or are designated as a point of contact for the security incident provided to CISA and (2) individuals who are involved in the security incident.

For both categories of individuals, this project receives names and contact information (e.g., phone numbers, email addresses, addresses).

For individuals involved in the incident, CISA may also receive:

- Images of the individuals involved in the incident (such images can be obtained by the facility's closed-circuit TV (CCTV) or security footage);
- Images of documents collected by the facility;
- Identification cards (which could be either legal or suspicious/fraudulent) collected by the facility from the individuals involved in the suspicious activity incident;
- Internal or local government reports about the incident obtained by the facility; and
- Additional types of PII, though less common, could include a physical description of the individuals involved in the incident, pictures, and video of the incident.

2.2 What are the sources of the information and how is the information collected for the project?

Information is primarily provided by facility security officers at the facility where the incident occurred. While it is difficult to provide an all-inclusive list of pathways or sources about

incident information, the most common pathways[17] by which information is collected are:

- An initial phone call from the facility security officer to a CSI. The facility security officer usually follows up the initial phone call with an email to the CSI describing the events in more detail. The email may contain attachments including, internal facility security reports, police reports, and photos. The CSI in turn provides the security incident information to Chemical Security;
- A facility security officer calls or emails CISA Central with a description of the incident. CISA Central forwards the incident to Chemical Security and the appropriate CSI. The CSI may reach out to the facility. During the subsequent contact, the facility may provide additional information about the security incident;
- A federal employee at another department or agency becomes aware of a security incident during the course of their normal duties. Generally, the federal employee contacts CISA via email or phone call. As appropriate, a CSI may reach out to the facility. During the subsequent contact, the facility may provide additional information about the security incident.

2.3 Does the project use information from commercial sources or publicly available data? If so, explain why and how this information is used.

This project does not use information from commercial sources or publicly available data.

2.4 Discuss how accuracy of the data is ensured.

Chemical Security reviews the information submitted and if Chemical Security has concerns about the accuracy of the incident information, it contacts the appropriate CISA Region and requests its CSI contact the facility security officer to resolve.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Privacy Risk: There is a risk that information received about an individual who is the subject of a SAR may not be accurate because the PII is not always collected directly from the individual involved.

Mitigation: This risk is partially mitigated. Considering that the personal information received on individuals involved in or related to a suspicious activity is not always voluntarily provided to the individual taking a security incident report, Chemical Security manages this risk

[17] Other less common potential pathways for incident information to be received by CISA, include the CFATS TipLine (https://www.cisa.gov/report-cfats-violation) and the CFATS Helpdesk.

by performing quality control reviews to verify accuracy of data. Investigations and verifications of the reported information are completed in a diligent manner, through employee training on responsible steps to ensure that sufficient and relevant details have been captured, and that the appropriate authorities (i.e., law enforcement or state and local entities) are notified to mitigate any potential hazard. Additionally, Chemical Security employees who are involved in evaluating incidents for consideration as a SAR will be properly trained on the ISE SAR Functional Standard. When a trained Chemical Security employee reviews the incident information, they will exercise personal judgment based upon a combination of knowledge, experience, and available information, to determine whether the information has a potential nexus to terrorism. Only those incidents that meet the ISE SAR Functional Standard will have the ISE-SAR data entered into eGuardian.

Section 3.0 Uses of the Information

3.1 Describe how and why the project uses the information.

Chemical Security collects incident information to identify those security incidents that meet the ISE SAR Functional Standard, have a potential nexus to terrorism, and are appropriate to be submitted into eGuardian. Chemical Security uses the information obtained to analyze risks to chemical facilities, track threat trends, and look for commonalities among threat actors.

3.2 Does the project use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how DHS plans to use such results.

This project does not use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate predictive patterns or anomalies.

3.3 Are there other components with assigned roles and responsibilities within the system?

This project shares incident information with other components or divisions within CISA in the event that:

- The incident is related to cybersecurity, the incident report will be shared via email with the CISA Region and Cyber Security Division;
- The report is related to explosives or explosive precursors, the incident report will be shared via email with the CISA Region and ISD's Office of Bombing Prevention; or

- The incident is related to a sector or area with other DHS components (e.g., Transportation Security Agency (TSA), U.S. Customs and Border Protection (CBP), U.S. Coast Guard (USCG)), the incident report will be shared with the component that has jurisdiction.

3.4 Privacy Impact Analysis: Related to the Uses of Information

Privacy Risk: There is risk of unauthorized access to the information.

Mitigation: This risk is mitigated. Incident reports are only accessible by those Chemical Security and CISA Regional personnel whose official duties give them the appropriate authority to review. All personnel who review the incident reports, from the time that they are reported to the time in which an official determination is made as to whether the incident warrants reporting into eGuardian, have received the necessary background checks and clearances, and have job responsibilities appropriate to handling such information. Additionally, when security incidents are received via telephone and/or email, only those CISA personnel with the appropriate "need to know" have access to the information. Further, access controls are in place to secure access to the security incident log stored on the shared drive.

Section 4.0 Notice

4.1 How does the project provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

This project does not routinely provide notice to either: (1) the individual submitting the incident information, or (2) the individual(s) involved in or considered a subject of the incident. CISA intends to provide notice through publication of this PIA. However, as appropriate, CSIs will respond to individuals submitting incident information to acknowledge receipt and include a statement notifying them that any PII provided as part of the emailed or telephone report may be included in the record of the incident.

4.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the project?

With regard to the information collected on an individual who is submitting incident information, those individuals generally have an ongoing business or official relationship with the chemical facility and/or the CSI, and thus the collection of the individual's information has likely already occurred during previous exchanges related to compliance with CFATS.

Individuals involved in or who are the subjects of security incidents at CFOIs do not have the opportunity to consent to how their information is used or opt out of the project prior to

submission of the incident information. Therefore, CISA is providing notice by way of this PIA and the forthcoming CISA SAR SORN. The project does expect CFOIs to comply with applicable local, state, and federal laws when collecting information about individuals that are involved in security incidents at CFOIs.

4.3 Privacy Impact Analysis: Related to Notice

Privacy Risk: There is a risk that the individuals whose personal information is captured in security incident reports will not receive notice prior to the collection.

Mitigation: This risk is partially mitigated. When appropriate, CISA provides notice to the reporting entities at the time a security incident is reported to inform them as to how their contact information will be used. In the instances that an individual's PII is captured during a security incident (e.g., via CCTV or surveillance camera), notice is commonly provided, via signage, at facilities to inform individuals that the grounds are monitored. Given the nature of SARs, individuals are typically not provided notice when they are the subject of a SAR. Providing direct notice to an individual may be harmful to intelligence or law enforcement activities. Therefore, CISA provides notice by way of this PIA, and the DHS/NPPD-001 National Infrastructure Coordinating Center (NICC) Records System temporarily until the forthcoming CISA SAR SORN is published.

Section 5.0 Data Retention by the Project

5.1 Explain how long and for what reason the information is retained.

Records created by CISA, such as security incident reports, are considered official communications and thus covered under the General Records Schedule and retained for seven years. If the security incident meets the ISE SAR Functional Standard and is submitted into eGuardian, then the record retention schedule for the SAR will be governed by the record retention schedule applicable to eGuardian (see the eGuardian PIA, N1-065-11-040[18]).

5.2 Privacy Impact Analysis: Related to Retention

Privacy Risk: There is the risk that PII may be retained in the system for a longer period than the purpose for which the information was collected requires.

Mitigation: This risk is mitigated. Records created by CISA, such as security incident reports, are considered official communications and thus covered under the General Records Schedule and retained for seven years. CISA will ensure adherence to the records schedule by conducting an annual review and a manual purge of security incident reports that have met the

[18] *See supra* note 17.

retention threshold. If the security incident meets the ISE SAR Functional Standard and is submitted into eGuardian, then the record retention schedule for the SAR will be governed by the record retention schedule applicable to eGuardian.

Section 6.0 Information Sharing

6.1 Is information shared outside of DHS as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.

Yes. Incident information meeting the ISE SAR Functional Standard will be submitted into eGuardian. On occasion, and based on "need to know," incident information also will be shared with other federal and state agencies located in the applicable regions which share security interests. Examples are the Occupational Safety and Health Administration, the Environmental Protection Agency, State Environmental Offices, State Offices of Emergency Management, and State Law Enforcement Officials.

6.2 Describe how the external sharing noted in 6.1 is compatible with the SORN noted in 1.2.

Chemical Security expects the majority of external sharing to occur under the authority of Routine Use K of the DHS/NPPD-001 NICC SORN, which allows this project to share incident information through eGuardian in compliance with the NSI.

6.3 Does the project place limitations on re-dissemination?

The project does not place any limitations on the re-dissemination of incident information.

6.4 Describe how the project maintains a record of any disclosures outside of the Department.

Incident information meeting the ISE SAR Functional Standard is submitted into eGuardian. eGuardian automatically assigns a unique incident number that will be used to maintain a record of disclosures outside of DHS.

If incident information must be shared outside of DHS and outside of eGuardian (either in addition to or instead of), when possible, the incident information will be transmitted via an encrypted data network. The project will maintain a record when information is shared externally from DHS. Depending on the urgency, information may occasionally be transmitted by secure email, in person, in paper format, by facsimile, by telephone, or otherwise as required by the circumstances necessitating such sharing.

6.5 Privacy Impact Analysis: Related to Information Sharing

Privacy Risk: There is a risk that information will be shared outside of DHS for a purpose inconsistent with the original collection.

Mitigation: This risk is mitigated. All PII collected, maintained, used, and disseminated by CISA during the security incident and SAR processes is covered by the Privacy Act. As such, information may only be disseminated consistent with the routine uses in the current DHS/NPPD-001 NICC SORN and forthcoming CISA SAR SORN. CISA does not share information externally in a manner inconsistent with the Privacy Act.

Section 7.0 Redress

7.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to any record containing information that is part of a DHS system of records may submit a Freedom of Information Act (FOIA) request to the DHS/CISA FOIA Officer. U.S. citizens, lawful permanent residents, and individuals who have records covered under the Judicial Redress Act (JRA) may file a Privacy Act (PA) request to access their information. Individuals may obtain instructions on how to submit a FOIA/PA request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homelandsecurity. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

The release of information is subject to standard FOIA and PA exemptions and, given the nature of the SAR information, CISA may not always permit individuals to gain access to their record(s).

7.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals seeking correction to any record containing information that is part of a DHS

system of records may submit a PA request to the DHS/CISA FOIA Officer. Individuals may obtain instructions on how to submit a PA request at https://www.dhs.gov/how-submit-foia-or-privacy-act-request-department-homelandsecurity. Please write to:

CISA FOIA Officer
245 Murray Lane SW
Washington, D.C. 20528-0380

Individuals may also make information inquiries to CISAFOIA@hq.dhs.gov.

However, given the nature of the incident report process, individuals may not be able to access and correct information about themselves given the investigatory nature of the records. Doing so could impede such an investigation. Notwithstanding, individuals may provide updated and corrected information that the project will incorporate into its records by sending information to CFATS@cisa.dhs.gov.

7.3 How does the project notify individuals about the procedures for correcting their information?

This PIA and the above-mentioned SORNs notify individuals about the procedures for correcting their information. However, due to the nature of the incident report process, individuals may not be able to correct information about themselves given the investigative nature of the records.

7.4 Privacy Impact Analysis: Related to Redress

Privacy Risk: There is a risk that inaccurate information will be collected on the subjects of the incidents without their consent or verification of accuracy.

Mitigation: This risk is partially mitigated. This PIA and the forthcoming CISA SAR SORN describe how individuals can make access requests under FOIA or the Privacy Act. While incidents are reported based on the information that is observed, received, and/or gathered at the time of the incident, the information generally cannot be updated. However, supplemental information can be added to the incident report or SAR.

Section 8.0 Auditing and Accountability

8.1 How does the project ensure that the information is used in accordance with stated practices in this PIA?

CISA has well-established and comprehensive information handling processes to enhance information security and eliminate possibilities for inappropriate sharing, misuse, and/or loss,

including the information handling processes described in the Department's Handbook for Safeguarding Sensitive Personally Identifiable Information.[19] Chemical Security and CISA Regional personnel participating in this project will adhere to established internal information security policies, as well as those outlined in CISA information technology security documents. Periodic audits and evaluations will ensure continued compliance with CISA security and privacy requirements, including those that cover the internal sharing of PII, and annual self-audits conducted by all DHS participants in the NSI. Chemical Security has developed and adheres to internal processes and Standard Operating Procedures specific to incident reporting.

8.2 Describe what privacy training is provided to users either generally or specifically relevant to the project.

All Chemical Security and CISA Regional personnel participating in this project must have a "need to know" to perform their duties and the authorization to handle the incident information. These individuals will be required to complete DHS privacy training on at least an annual basis.

All Chemical Security and CISA Regional personnel evaluating incidents for consideration as a SAR will be properly trained on the criteria in the ISE SAR Functional Standard.

8.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

CISA personnel who have access to the initial security incident report, as well as the personnel who determine whether the incident meets the criteria outlined in the ISE SAR Functional Standard, must possess the necessary security clearances and be authorized access per their official duties.

Incident information is generally received by the project via email when a chemical facility contacts CISA. Upon receipt, incident information is stored in an access-restricted folder on a shared drive. Only authorized individuals within Chemical Security with direct responsibility to enter SAR into eGuardian have eGuardian accounts.

8.4 How does the project review and approve information sharing agreements, Memoranda of Understanding (MOUs), new uses of the information, new access to the system by organizations within DHS and outside?

All MOUs are reviewed by the program manager, CISA Privacy Officer, and legal counsel,

[19] *See* U.S. DEPARTMENT OF HOMELAND SECURITY, HANDBOOK FOR SAFEGUARDING SENSTIVE PII (2017), *available at* https://www.dhs.gov/privacy-policy-guidance.

and then sent to DHS for formal review.

Contact Official

Lona Saccomando
Deputy Branch Chief, Chemical Security Subdivision
Infrastructure Security Division/ Cybersecurity and Infrastructure Security Agency
CFATS@hq.dhs.gov

Responsible Official

David Wulf
Associate Director, Chemical Security Subdivision
Infrastructure Security Division/Cybersecurity and Infrastructure Security Agency

Approval Signature

Original, signed copy on file at the DHS Privacy Office.

_____

Dena Kozanas
Chief Privacy Officer
U.S. Department of Homeland Security
(202) 343-1717